

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52

(10) 国際公開番号
WO 2004/010662 A1

- [illegible]

- (57) 要約: 電子メールサーバは、ユーザにとって不要な情報を発信するWebサイトのURLの一部分または全部を記憶する迷惑サイトデータベースと、DMの配信業者の端末装置から送信された電子メールを受信するメール受信部と、受信した電子メールの中に、迷惑サイトデータベースに記憶されているURLの一部分または全部が含まれているか否かを判別する迷惑メール判別部と、URLの一部分または全部が含まれていないと判別された場合にのみ電子メールをユーザの端末装置に送信するメール送信部とを備える。

明 細 書

電子メールサーバ、電子メールの受渡しの中継方法、およびコンピュータプログラム

5

技術分野

本発明は、ユーザにとって迷惑な電子メールがユーザの端末装置に送信されないように処理する電子メールサーバに関する。

10

背景技術

DM（ダイレクトメール）を電子メールによって配信することは、業者にとって次のようなメリットがある。まず、郵便や宅配便などによって配信する場合に比べて、コストを低く抑えることができるし、多くのユーザに配信してもほとんど手間が掛からない。また、電子メールに業者自身が開設するWebサイトのWebページのURLを記載しておけば、興味のあるユーザが自ら業者のWebサイトにアクセスしてくれるので、電子メールのデザインやレイアウトなどに特別な工夫を凝らす必要がなく電子メールの作成が簡単である。このようなメリットから、電子メールによってDMを配信する業者が非常に多い。

15

20

しかし、逆に、ユーザにとっては、このような電子メールを受け取ることが迷惑である場合が多い。なぜなら、電子メールを受け取るたびに、その内容に目を通して必要な電子メールであるか否かを判別しなければならず、無駄な時間が掛かってしまうからである。電子メールに記載されているURLに基づいてWebサイトにアクセスしなければ、必要な電子メールであるか否かを判別できない場合もある。また、電子メールの内容そのものがユーザにとって不快な場合がある。さらに、携帯電

25

話のユーザは、電子メールを受け取るたびに通信料を支払わなければならない場合があり、費用が嵩む。

そこで、ユーザが指定した特定の相手からの電子メールの受取りを拒否する方法が提案されている。例えば、ユーザは、頻繁にDMを送信して
5 くる業者の電子メールアドレスまたはドメイン名をISP (Internet Service Provider) の電子メールサーバに登録しておく。電子メールサーバは、そのユーザ宛ての電子メールをフィルタに掛け、業者から送信された電子メールを抽出する。そして、抽出された電子メールを迷惑メールとみなし、ユーザの端末装置に送信せずに削除する。

10 ところが、最近では、送信元の電子メールアドレスを偽って迷惑メールを配信する業者が増えている。業者にとっては、自己のWebページのURLさえユーザに知らせることができればよいからである。したがって、せっかく電子メールサーバに業者の電子メールアドレスなどを登録しておいても、迷惑メールがフィルタを通過し、ユーザの端末装置に届
15 けられてしまう。

本発明は、このような問題点に鑑み、送信元の電子メールアドレスに関わらずユーザが迷惑メールの受取りを拒否することができるようにすることを目的とする。

20 発明の開示

本発明に係る電子メールサーバは、電子メールの受渡しの中継を行う電子メールサーバであって、電子メールの受取人にとって不要な情報を発信するWebサイトのURLの一部分または全部を記憶する迷惑URL記憶手段と、差出人の端末装置から送信された電子メールを受信する
25 受信手段と、受信した電子メールの中に前記迷惑URL記憶手段に記憶されている前記URLの一部分または全部が含まれているか否かを判別

する判別手段と、前記URLの一部分または全部が含まれていないと判別された場合にのみ、前記受信した電子メールを当該電子メールの受取人の端末装置に送信する送信手段とを有してなる。

5 好ましくは、URLを決める際のドメインのドメイン名と各ドメインに設けられるWebサイトのサイト名との関係を示すURL規則情報を記憶するURL規則記憶手段と、受け取ったユーザにとって迷惑な電子メールである迷惑メールを当該ユーザの端末装置から受信する第一の受信手段と、受信した迷惑メールに含まれるURLに示されるドメイン名を抽出するドメイン抽出手段と、抽出されたドメイン名から前記URL規則情報を参照して、前記受信した迷惑メールに含まれるURLに示されるWebページを配信するWebサイトを特定するWebサイト特定手段と、抽出されたドメイン名と特定されたWebサイトのサイト名とを迷惑サイト情報として前記ユーザと対応付けて記憶する迷惑サイト記憶手段と、差出人の端末装置から送信された電子メールを受信する第二の受信手段と、受信した電子メールに含まれるURLの中に当該電子メールの宛先であるユーザの前記迷惑サイト情報に示されるドメイン名およびサイト名が含まれているか否かを判別することによって、当該電子メールが迷惑メールであるか否かを判別する迷惑メール判別手段と、前記受信した電子メールが迷惑メールでないと判別された場合にのみ、当該電子メールを宛先であるユーザの端末装置に送信する送信手段とを有してなる。

25 または、前記第一の受信手段によって受信された迷惑メールに含まれるURLに示されるWebページを取得する第一のWebページ取得手段を有し、前記第一のWebページ取得手段によって取得されたWebページの中に他のWebページに自動的にジャンプするコードが含まれている場合に、前記ドメイン抽出手段は、当該他のWebページが設け

られるドメインのドメイン名を抽出し、前記Webサイト特定手段は、当該他のWebページを配信するWebサイトを特定し、前記迷惑サイト記憶手段は、当該他のWebページを配信するWebサイトが設けられるドメインのドメイン名と当該Webサイトのサイト名とを迷惑サイト情報として記憶する。

または、前記第二の受信手段によって受信された電子メールに含まれるURLに示されるWebページを取得する第二のWebページ取得手段を有し、迷惑メール判別手段は、前記第二のWebページ取得手段によって取得されたWebページの中に他のWebページに自動的にジャンプするコードが含まれている場合に、当該他のWebページのURLに基づいて前記電子メールが迷惑メールであるか否かを判別する。

本発明に係る電子メールの受渡しの中継方法は、電子メールの受取人にとって不要な情報を発信するWebサイトのURLの一部分または全部を記憶しておき、差出人の端末装置から送信された電子メールを受信し、受信した電子メールの中に、記憶しておいた前記URLの一部分または全部が含まれているか否かを判別し、前記URLの一部分または全部が含まれていないと判別された場合にのみ、前記受信した電子メールを当該電子メールの受取人の端末装置に送信する。

図面の簡単な説明

図1は、本発明に係る電子メールサーバが設けられた電子メールシステムの構成の例を示す図である。

図2は、URLの規則のパターンの例を説明する図である。

図3は、電子メールサーバのハードウェア構成の例を示す図である。

図4は、電子メールサーバの機能的構成の例を示す図である。

図5は、URL規則データベースの構成の例を示す図である。

図 6 は、迷惑サイトデータベースの構成の例を示す図である。

図 7 は、配信業者からユーザに宛てて送信された電子メールの例を示す図である。

図 8 は、一般的な URL の規則の例を説明する図である。

5

図 9 は、Web ページのリダイレクトの機能の仕組みを説明する図である。

図 10 は、リダイレクトのコードを有する HTML ファイルの例を示す図である。

10

図 11 は、電子メールの受渡しの中継を行う際の処理の流れの例を説明するフローチャートである。

図 12 は、迷惑サイトの登録を行う際の処理の流れの例を説明するフローチャートである。

発明を実施するための最良の形態

15

図 1 に示すように、本発明に係る電子メールサーバ 1 は、通信回線 4 を介して端末装置 2、3 および WWW サーバ 5 などの装置に接続することができる。通信回線 4 として、インターネット、LAN、専用線、または公衆回線などが用いられる。

20

端末装置 3 には、電子メールの作成および送受信などを行うための電子メールソフトおよび Web ページを閲覧するための WWW ブラウザなどがインストールされている。各端末装置 3 のユーザには、電子メールアドレスが 1 つずつ与えられている。ユーザは、電子メールサーバ 1 を SMTP (Simple Mail Transfer Protocol) サーバおよび POP (Post Office Protocol) サーバとして利用し、他のユーザと電子メールのやりとりをすることができる。端末装置 3 として、パーソナルコンピュータ、ワークステーション、PDA (Personal Digital Assistant)、

25

または携帯電話装置などが用いられる。

5 端末装置 2 は、電子メールによって D M（ダイレクトメール）を無差別に配信する業者の端末装置である。D M には、この配信業者の商品またはサービスなどの宣伝のほか、この配信業者が開設している W e b サイトの U R L などが記載されている。ここでは、このような電子メールを「迷惑メール」または「スパムメール」と呼ぶことにする。配信業者は、多数のユーザの電子メールアドレスを知得しており、これらの電子メールアドレスを宛先として指定し、迷惑メールを送信する。

10 I S P（Internet Service Provider）または企業などには、それぞれ、「xxxxx.ne.jp」のようなドメイン名のドメインが与えられている。ドメインには、会員数、アクセス数、または配信する情報量などに応じて 1 つまたは複数の W W W サーバ 5 が設けられている。このような構成により、ドメインには、1 つまたは複数の W e b サイト（W W W サイト）が設けられている。

15 例えば、I S P のドメインの場合は、個人会員または法人会員ごとの W e b サイトが設けられている。各 W e b サイトにはサブドメインまたはディレクトリが与えられており、他の W e b サイトと区別するためのサイト名が付けられている。

20 U R L（Uniform Resource Locator）の決め方すなわち W e b サイトのサイト名の付け方はドメインごとにそれぞれ異なり、図 2 に示すようなパターンに大別される。例えば、「サブドメイン名.xxxxx.ne.jp」のようにドメイン名の前のサブドメイン名をサイト名とするパターン A、「xxxxx.ne.jp/ディレクトリ名」のようにドメイン名の後のディレクトリ名をサイト名とするパターン B、「xxxxx.ne.jp/ディレクトリ名」
25 のようにディレクトリ名をサイト名とし、サイト名を表す記号として「～」（チルダ）を用いるパターン C、または「サブドメイン名.xxxxx.n

e.jp/ディレクトリ名」のようにサブドメイン名とディレクトリ名とを組み合わせ、サイト名とするパターンDなどがある。なお、パターンA、Dにおいて、サブドメイン名の代わりにWWWサーバ名が用いられる場合もある。

5 企業のドメインの場合は、本社、支社、または関連会社などのためのWebサイトが複数設けられている場合と自社の紹介のためのWebサイトが1つだけ設けられる場合とがある。前者の場合は、図2のパターンA～Dのようにサイト名が付けられる。後者の場合は、ドメイン名がサイト名として用いられる（パターンE）。

10 Webサイトの所有者は、原則として自由に自分のWebサイトの中にWebページを設けることができる。Webページは、HTML（Hypertext Markup Language）またはXML（Extensible Markup Language）などで記述される。DMの配信業者は、ISPの法人会員としてWebサイトを開設し、または独自のドメインを取得してWebサイトを開設している。

15 電子メールサーバ1は、図3に示すように、CPU1a、RAM1b、ROM1c、磁気記憶装置1d、および種々のインタフェースなどによって構成される。磁気記憶装置1dには、オペレーティングシステム（OS）、SMTPサーバ用プログラム、POPサーバ用プログラム、迷惑メールを検出するためのプログラム、および種々のデータなどが記憶されている。これらのプログラムまたはデータは、必要に応じてRAM1bにロードされ、CPU1aによってプログラムが実行される。

20 なお、電子メールサーバ1は、図1に示すように1台のサーバ機によって構成してもよいし、複数台のサーバ機に分散して構成してもよい。例えば、SMTPサーバの処理とPOPサーバの処理とをそれぞれ異なるサーバ機を用いて行うように構成してもよい。

このような構成によって、電子メールサーバ1は、図4に示すように、URL規則データベース1D1、迷惑サイトデータベース1D2、メールボックス1D3、メール受信部101、迷惑メール判別部102、メール送信部103、迷惑メール受信部104、ドメイン判別部105、
5 迷惑サイト特定部106、第一のリダイレクト先取得部107、および第二のリダイレクト先取得部108などの機能が実現される。

URL規則データベース1D1は、図5に示すように、インターネット上のドメインごとにURLの付け方の規則性を示すURL規則情報71（71a、71b、…）を記憶している。メールボックス1D3は、
10 端末装置3のユーザごとに設けられており、インターネット上の端末装置から送信されたそのユーザ宛ての電子メール70を一時的に格納しておく。

迷惑サイトデータベース1D2は、図6に示すように、ユーザごとにそのユーザにとって意義のない不必要な情報を配信するWebサイトを示す迷惑サイト情報72（72a、72b、…）を記憶している。以下、
15 このようなWebサイトを「迷惑サイト」と記載することがある。迷惑サイト情報72に登録されているWebサイト（迷惑サイト）は、ユーザが受け取った迷惑メールの文書の中に記載されていたURLに基づいて登録される。迷惑サイトを登録する方法については、後に説明する
20 。

迷惑サイト情報72における迷惑サイトのURLの記述の形式は、上に述べたドメインのパターン（図5参照）によってそれぞれ異なる。例えば、パターンAを採用するドメインに開設されているWebサイトの場合は、「ppp.bbbbbb.ne.jp」のように「サイト名（サブドメイン名）
25 +ドメイン名」という形式で記述される。パターンEを採用するドメインの場合は、ドメイン全体で1つのWebサイトを形成するので、「aa

aaa.co.jp」のようにドメイン名だけでサイト名を表す。

メール受信部 101 は、インターネット上の種々の端末装置から送信された電子メールのうち、端末装置 3 のユーザに宛てた電子メール 70 を受信する。電子メール 70 には、DM の配信業者の端末装置 2 から送信された迷惑メールが含まれている場合がある。

迷惑メール判別部 102 は、受信した電子メール 70 が迷惑メールであるか否かを判別する。係る判別は、次のようにして行われる。まず、電子メール 70 の本文の中に記載されている URL を抽出する。例えば、図 7 (a) に示す電子メール 70 a の場合は、「http://www.ppp.bbb.bb.ne.jp/top.html」が抽出される。

電子メール 70 の宛先に記載されたユーザの迷惑サイト情報 72 に示される迷惑サイトのうちのいずれかが、抽出された URL の全部または一部分と一致するか否かを判別する。ユーザ A に宛てた電子メール 70 a の場合は、図 6 の迷惑サイト情報 72 a に示す 5 つの迷惑サイトのうちの「ppp.bbbbbb.ne.jp」が、抽出された URL の一部分と一致する。一致した場合は、その電子メール 70 a を迷惑メールであると判別する。これに対して、図 7 (b) の電子メール 70 b のように、迷惑サイト情報 72 a に示されるいずれの迷惑サイトも本文中の URL の全部または一部分と一致しない場合は、その電子メール 70 b は、通常の電子メールであると判別される。

図 4 に戻って、メール送信部 103 は、通常の電子メールと判別された電子メール 70 を、宛先のユーザの端末装置 3 に送信する。端末装置 3 が携帯電話装置である場合は、電子メール 70 が通常の電子メールであると判別されたタイミングで送信を行う。端末装置 3 がパーソナルコンピュータである場合は、一旦、電子メール 70 をそのユーザのメールボックス 1D3 に格納しておく。そして、端末装置 3 から要求があった

タイミングで送信を行う。

迷惑メールと判別された電子メール 70 は、ユーザに届けられることなく削除される。ただし、直ちに削除するのではなく、そのユーザのメールボックス 1 D 3 に通常の電子メールと区別して一時的に格納してお

5 いてもよい。これにより、ユーザは、迷惑メールが削除される前に、迷惑メールの内容を念のために確認することができる。この場合、迷惑メールは、ユーザから指令があった場合または所定の期間の経過後にメールボックス 1 D 3 から削除される。

迷惑サイト情報 7 2 に登録されている Web サイト（迷惑サイト）の URL が 1 つも記載されていない電子メール 70 は、たとえそれが迷惑

10 メールであったとしても、端末装置 3 に届けられてしまう。そこで、ユーザは、今後、係る迷惑サイトを案内する迷惑メールが届けられないように電子メールサーバ 1 に対して要求することができる。

ユーザは、端末装置 3 を操作して、配信業者から受け取った電子メール 70 （迷惑メール）を電子メールサーバ 1 に転送する。例えば、図 7

15 （b）の電子メール 70 b を転送する。

電子メールサーバ 1 において、迷惑メール受信部 104 が端末装置 3 から迷惑メールを受信すると、ドメイン判別部 105 は、この迷惑メールに記載されている URL からドメイン名を抽出する。これにより、URL が指す Web ページを配信する Web サイト（迷惑サイト）の属

20 するドメインが判別される。一般に、URL は、図 8 のような規則に基づいて付けられている。したがって、電子メール 70 b の場合は、「dddd d.com」というドメイン名が抽出（判別）される。

迷惑サイト特定部 106 は、抽出されたドメインに対応する URL 規則情報 7 1 に基づいて、迷惑メールに記載されている URL が指す Web サイトを特定する。電子メール 70 b に記載されている URL の場合

25

は、図 5 に示すドメイン「dddddd.com」のURL規則情報 7 1 d より、ドメイン名の後にサイト名が記載されていることが分かる。したがって、Web サイトは「abcde」であると特定される。

5 特定されたWeb サイトは、迷惑メールの転送元であるユーザにとつての迷惑サイトとみなされ、そのユーザの迷惑サイト情報 7 2 に追加（登録）される。Web サイト（迷惑サイト）は、そのWeb サイトの属するドメインのURL規則情報 7 1 に示される規則に従って、サイト名とドメイン名とを含むように登録される。例えば、上記のWeb サイト「abcde」の場合は、図 5 のURL規則情報 7 1 d に従って「dddddd.com
10 /abcde」のように登録される。ただし、1つのドメインにWeb サイトが1つだけ形成されている場合は、ドメイン名がそのWeb サイトのサイト名を表していることになる。したがって、「aaaaa.co.jp」のようにドメイン名が迷惑サイト情報 7 2 に登録される。

15 以上の処理によって、ユーザは、今後、自分の迷惑サイト情報 7 2 に登録した迷惑サイトのURLを案内する迷惑メールの受取りを拒否することができる。

図 9 はWeb ページのリダイレクトの機能の仕組みを説明する図、図 10 はリダイレクトのコードを有するHTML ファイルの例を示す図である。ところで、HTML またはXML などのリダイレクトの機能を使用すると、配信業者は、ユーザに配信する電子メール 7 0 に自社のWeb
20 サイトのURLを直接記載することなく、自社のWeb サイトをユーザに閲覧させることができる。これは、図 9 に説明するような仕組みによる。

25 例えば、配信業者は、図 9（a）に示すような電子メール 7 0 c を配信する。端末装置 3 は、受信された電子メール 7 0 c に記載されているURLがクリックされると、WWWブラウザを起動し、図 9（b）に示

5 すようにダミーのWebサイト5aからWebページ74（HTMLファイル）をダウンロードする。このHTMLファイルには、図10に示すようにリダイレクト（ジャンプ）のコードであるタグC1が含まれている。したがって、端末装置3は、タグC1に基づいて配信業者の真のWebサイト5bにアクセスし直し（リダイレクトし）、Webページ75をダウンロードする。

10 配信業者は、いわゆる無料プロバイダなどを利用してWebサイト5aのようなダミーのWebサイトを次々に新規作成し、図9(a)のURLを頻繁に変更しながらユーザに迷惑メールを配信する。したがって、ユーザは、図6に示す迷惑サイト情報72にWebサイト5aを登録しても、配信業者の真のWebサイト5bを間接的に案内する迷惑メールの受取りを拒否することができない。そこで、電子メールサーバ1は、このような手段に対処するために、次のような処理を行う。

図４の第一のリダイレクト先取得部１０７は、ユーザの端末装置３から転送されてきた電子メール７０に記載されているＵＲＬに基づいてＷｅｂページを取得する。取得されたＷｅｂページの中からリダイレクトのコードを検索する。そして、リダイレクトのコードがあった場合は、そのコードに示されるリダイレクト先のＵＲＬを抽出する。例えば、図１０に示すＨＴＭＬファイルがＷｅｂページとして取得された場合は、タグＣ１に示されるＵＲＬ「http://www.ppp.bbbbbb.ne.jp/top.html」を抽出する。

ドメイン判別部 105 は、抽出された URL が指す Web ページを配信する Web サイトの属するドメインを判別する。迷惑サイト特定部 106 は、この Web サイトのサイト名を特定する。これらの処理によって、この Web サイトは迷惑サイトとみなされ、迷惑メールの転送元であるユーザの迷惑サイト情報 72 に登録される。

一方、第二のリダイレクト先取得部 108 は、配信業者から送信された電子メール 70 の本文中に記載されている URL が指す Web ページを取得する。迷惑メール判別部 102 は、取得された Web ページに記載されているリダイレクトのコード（例えば図 10 に示すタグ C1）からリダイレクト先の URL を抽出する。そして、抽出された URL および宛先のユーザの迷惑サイト情報 72 に基づいて、電子メール 70 が迷惑メールであるか否かを判別する。迷惑メールでないと判別された電子メール 70 は、宛先のユーザの端末装置 3 に送信される。迷惑メールであると判別された電子メール 70 は、削除され、または通常の電子メールと区別して所定の期間だけメールボックス 1D3 に保存される。

次に、電子メールサーバ 1 の処理の流れを、フローチャートを参照して説明する。図 11 は電子メールの受渡しの中継を行う際の処理の流れの例を説明するフローチャート、図 12 は迷惑サイトの登録を行う際の処理の流れの例を説明するフローチャートである。

図 11 において、例えば、配信業者が送信したユーザ A 宛ての電子メール 70 を受信すると（#11）、この電子メール 70 に記載されている URL を抽出し（#12）、抽出された URL およびユーザ A の迷惑サイト情報 72a に基づいてこの電子メール 70 が迷惑メールであるか否かを判別する（#13）。迷惑メールであると判別された場合は（#13 で Yes）、電子メール 70 を削除する（#19）。または、ユーザ A のメールボックス 1D3 に通常の電子メールと区別して保存しておき、所定の期間が経過した後に削除する。

迷惑メールでないと判別された場合は（#13 で No）、電子メール 70 をユーザ A の端末装置 3 に送信する（#18）。ただし、電子メール 70 は、図 9（b）に示すような手段によって配信業者の Web サイト（Web サイト 5b）を間接的に案内する迷惑メールである可能性が

ある。そこで、ステップ# 18を行う前に、次のような処理を行ってもよい。

5 ステップ# 12で抽出されたURLが指すWebページを取得し（# 14）、このWebページの中に他のWebページへリダイレクト（ジャンプ）するコードが含まれているか否かを判別する（# 15）。

10 係るコードが含まれていない場合は、電子メール70をユーザAの端末装置3に送信する（# 18）。含まれている場合は、係るコードからリダイレクト先（ジャンプ先）のURLを抽出し（# 16）、ステップ# 13と同様に電子メール70が迷惑メールであるか否かを判別し（# 17）、判別結果に応じて電子メール70を削除し（# 19）またはユーザAの端末装置3に送信する（# 18）。

15 ユーザが受け取った電子メール70に案内されているWebページ（Webサイト）を迷惑サイトとして登録する場合は、図12のような手順で処理が行われる。電子メールサーバ1は、例えば、図7（b）に示すような電子メール70bをユーザAから受け取ると（# 21）、その電子メール70bに記載されているURL「http://dddd.com/~abcde/index.html」を抽出し（# 22）、そのURLが示すWebページを配信しているWebサイト（迷惑サイト）およびその迷惑サイトの属するドメインを特定する（# 23）。そして、特定されたドメインのドメイン名および迷惑サイトのサイト名に基づいて迷惑サイト「dddd.com/~abcde」をユーザAの迷惑サイト情報72aに登録する（# 24）。

20 ステップ# 23、# 24の処理と前後してまたは並行して、ステップ# 22で抽出されたURLが指すWebページ（HTMLファイルなど）を取得する（# 25）。取得したWebページの中に、他のWebページへリダイレクト（ジャンプ）するコードが含まれているか否かを判別する（# 26）。係るコードが含まれている場合は（# 26でYes

）、ステップ# 2 2～# 2 4と同様に、リダイレクト先を示すURLに基づいて迷惑サイトをユーザAの迷惑サイト情報7 2 aに登録する（# 2 7～# 2 9）。

5 なお、迷惑メールに示されるURLから最終的な迷惑サイト（例えば、図9（b）のWebサイト5 b）に辿り着くまでの間にリダイレクトのコードを有するダミーのWebページ（例えば、図9（b）のWebサイト5 a）が複数設けられている場合がある。このような場合に対処するために、リダイレクト先がないWebページ（すなわち最終的な迷惑サイト）に辿り着くまで、図11のステップ# 1 5～# 1 7の処理または図12のステップ# 2 7～# 2 9の処理を繰り返し行ってもよい。

10 本実施形態によると、ユーザは、ユーザ自身が迷惑だと感じる電子メールの受取りを、送信元の電子メールアドレスに関わらず拒否することができる。

15 本実施形態では、図6に示すようにユーザごとに迷惑サイト情報7 2を記憶しておいたが、全てのユーザに共通の迷惑サイト情報7 2を記憶しておいてもよい。例えば、多くのユーザによって迷惑サイトとみなされたWebサイトを共通の迷惑サイト情報7 2に登録しておく。または、公序良俗に反する情報を配信するWebサイトを、電子メールサーバ1の管理者が予め共通の迷惑サイト情報7 2に登録しておく。この共通の迷惑サイト情報7 2およびユーザ自身の迷惑サイト情報7 2の両方に基づいて迷惑メールであるか否かを判別することによって、より効率的に迷惑メールの受信を拒否することができる。特に、電子メールサーバ1の利用を開始して間もないユーザの場合は、自分の迷惑サイト情報7 2に登録されている迷惑サイトが少ないが、共通の迷惑サイト情報7 2を用いることによって、すぐに本サービスの効果を得ることができる。

25 その他、電子メールサーバ1、端末装置2、3の全体または各部の構

成、URL規則データベース1D1、迷惑サイトデータベース1D2などのデータベースの構成、処理内容、処理順序などは、本発明の趣旨に沿って適宜変更することができる。

5 産業上の利用可能性

以上のように、本発明による電子メールサーバは、迷惑サイトデータベースに登録されているWebページのURLが記載されている電子メールをユーザの端末装置に送信せずに削除するので、迷惑な電子メールをチェックする無駄な時間をなくして効率的に仕事を行うことができる環境をユーザに提供できる点で有用なものである。また、送信者の電子メールアドレスに関わらず電子メールが迷惑メールであるか否かを判別するので、送信者の電子メールアドレスを偽った電子メールであっても、迷惑な電子メールを削除することができるという点で有用なものである。

請 求 の 範 囲

1. 電子メールの受渡しの中継を行う電子メールサーバであって、

電子メールの受取人にとって不要な情報を発信するWebサイトのURLの一部分または全部を記憶する迷惑URL記憶手段と、

5

差出人の端末装置から送信された電子メールを受信する受信手段と、

受信した電子メールの中に前記迷惑URL記憶手段に記憶されている前記URLの一部分または全部が含まれているか否かを判別する判別手段と、

10

前記URLの一部分または全部が含まれていないと判別された場合にのみ、前記受信した電子メールを当該電子メールの受取人の端末装置に送信する送信手段と、

を有してなることを特徴とする電子メールサーバ。

2. 電子メールの受渡しの中継を行う電子メールサーバであって、

15

URLを決める際のドメインのドメイン名と各ドメインに設けられるWebサイトのサイト名との関係を示すURL規則情報を記憶するURL規則記憶手段と、

受け取ったユーザにとって迷惑な電子メールである迷惑メールを当該ユーザの端末装置から受信する第一の受信手段と、

20

受信した迷惑メールに含まれるURLに示されるドメイン名を抽出するドメイン抽出手段と、

抽出されたドメイン名から前記URL規則情報を参照して、前記受信した迷惑メールに含まれるURLに示されるWebページを配信するWebサイトを特定するWebサイト特定手段と、

25

抽出されたドメイン名と特定されたWebサイトのサイト名とを迷惑サイト情報として前記ユーザと対応付けて記憶する迷惑サイト記憶手段と、

差出人の端末装置から送信された電子メールを受信する第二の受信手段と、

5 受信した電子メールに含まれるURLの中に当該電子メールの宛先であるユーザの前記迷惑サイト情報に示されるドメイン名およびサイト名が含まれているか否かを判別することによって、当該電子メールが迷惑メールであるか否かを判別する迷惑メール判別手段と、

前記受信した電子メールが迷惑メールでないと判別された場合にのみ、当該電子メールを宛先であるユーザの端末装置に送信する送信手段と、

10 を有してなることを特徴とする電子メールサーバ。

3. 前記第一の受信手段によって受信された迷惑メールに含まれるURLに示されるWebページを取得する第一のWebページ取得手段を有し、

15 前記第一のWebページ取得手段によって取得されたWebページの中に他のWebページに自動的にジャンプするコードが含まれている場合に、

前記ドメイン抽出手段は、当該他のWebページが設けられるドメインのドメイン名を抽出し、

20 前記Webサイト特定手段は、当該他のWebページを配信するWebサイトを特定し、

前記迷惑サイト記憶手段は、当該他のWebページを配信するWebサイトが設けられるドメインのドメイン名と当該Webサイトのサイト名とを迷惑サイト情報として記憶する、

25 請求項2記載の電子メールサーバ。

4. 前記第二の受信手段によって受信された電子メールに含まれるURLに示されるWebページを取得する第二のWebページ取得手段を有

し、

迷惑メール判別手段は、前記第二のW e b ページ取得手段によって取得されたW e b ページの中に他のW e b ページに自動的にジャンプするコードが含まれている場合に、当該他のW e b ページのU R Lに基づいて前記電子メールが迷惑メールであるか否かを判別する、

請求項 2 または請求項 3 記載の電子メールサーバ。

5. 電子メールサーバにおける電子メールの受渡しの中継方法であって、

電子メールの受取人にとって不要な情報を発信するW e b サイトのU R L の一部分または全部を記憶しておき、

差出人の端末装置から送信された電子メールを受信し、

受信した電子メールの中に、記憶しておいた前記U R L の一部分または全部が含まれているか否かを判別し、

前記U R L の一部分または全部が含まれていないと判別された場合にのみ、前記受信した電子メールを当該電子メールの受取人の端末装置に送信する、

ことを特徴とする電子メールの受渡しの中継方法。

6. 電子メールの受渡しの中継を行うコンピュータに用いられるコンピュータプログラムであって、

差出人の端末装置から送信された電子メールを受信する処理と、

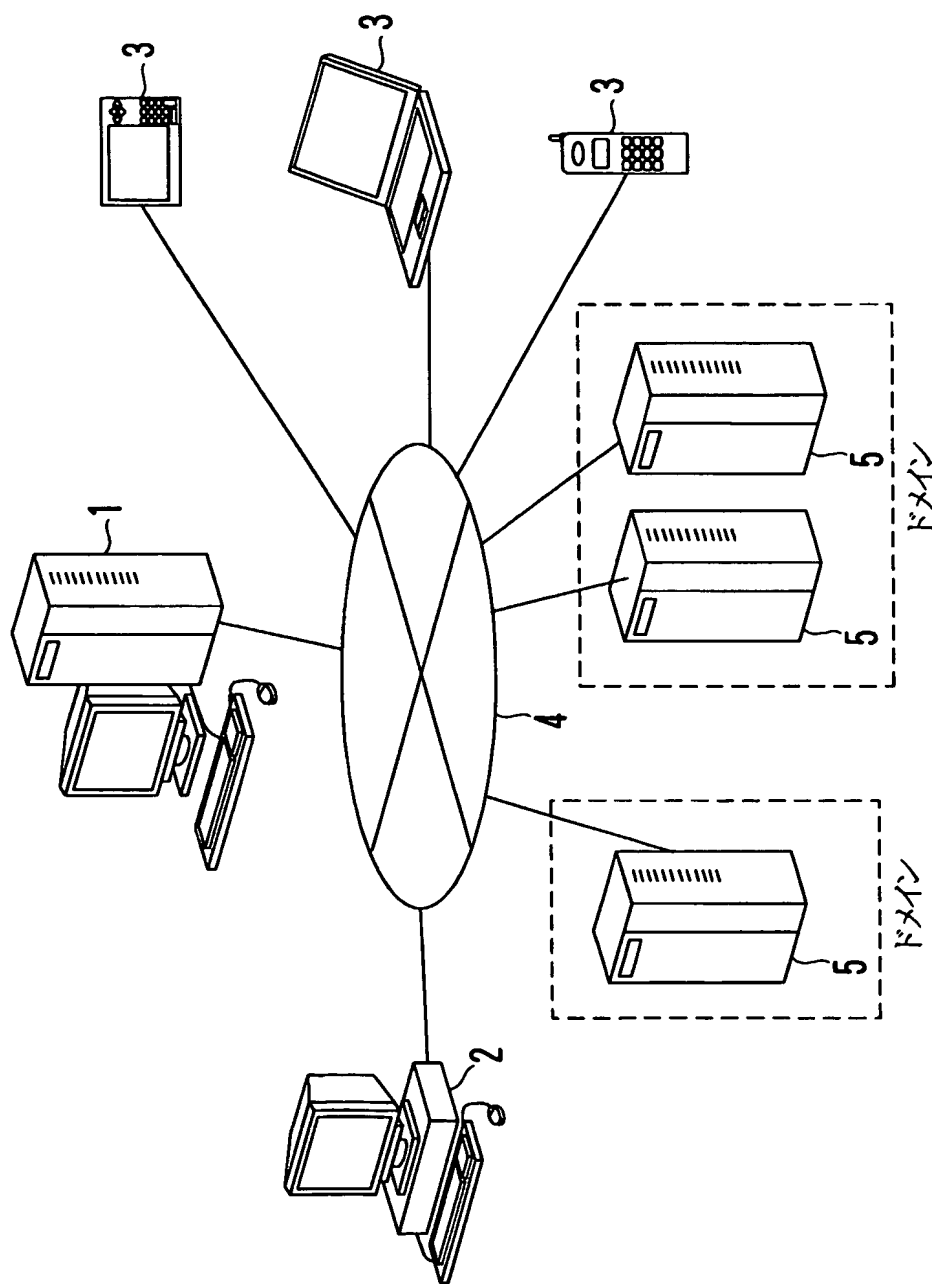
受信した電子メールの受取人にとって不要な情報を発信するW e b サイトのU R L の一部分または全部が、当該電子メールの中に含まれているか否かを判別する処理と、

前記U R L の一部分または全部が含まれていないと判別された場合にのみ、前記受信した電子メールを当該電子メールの受取人の端末装置に送信する処理と、

をコンピュータに実行させるためのコンピュータプログラム。

1/12

図1



2/12

図2

パターン	規則	サイト名
A	サブドメイン名(orWWWサーバ名).ドメイン名 例 http://website.xxxxx.ne.jp	サブドメイン名(orWWWサーバ名)
B	ドメイン名/ディレクトリ名 例 http://xxxxx.ne.jp/website	ディレクトリ名
C	ドメイン名/~ディレクトリ名 例 http://xxxxx.ne.jp/~website	ディレクトリ名
D	サブドメイン名(orWWWサーバ名).ドメイン名/ディレクトリ名 例 http://homepage3.xxxxx.ne.jp/website	サブドメイン名(orWWWサーバ名) +ディレクトリ名
E	ドメイン名 例 http://xxxxx.co.jp	ドメイン名
⋮	⋮	⋮

3/12

図3

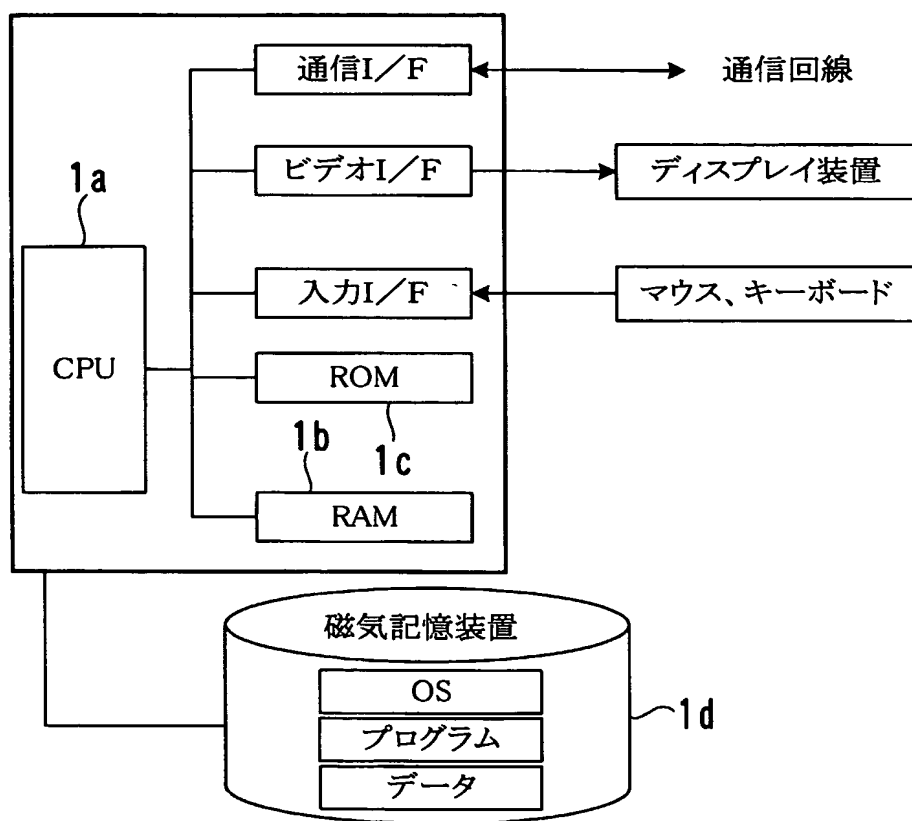
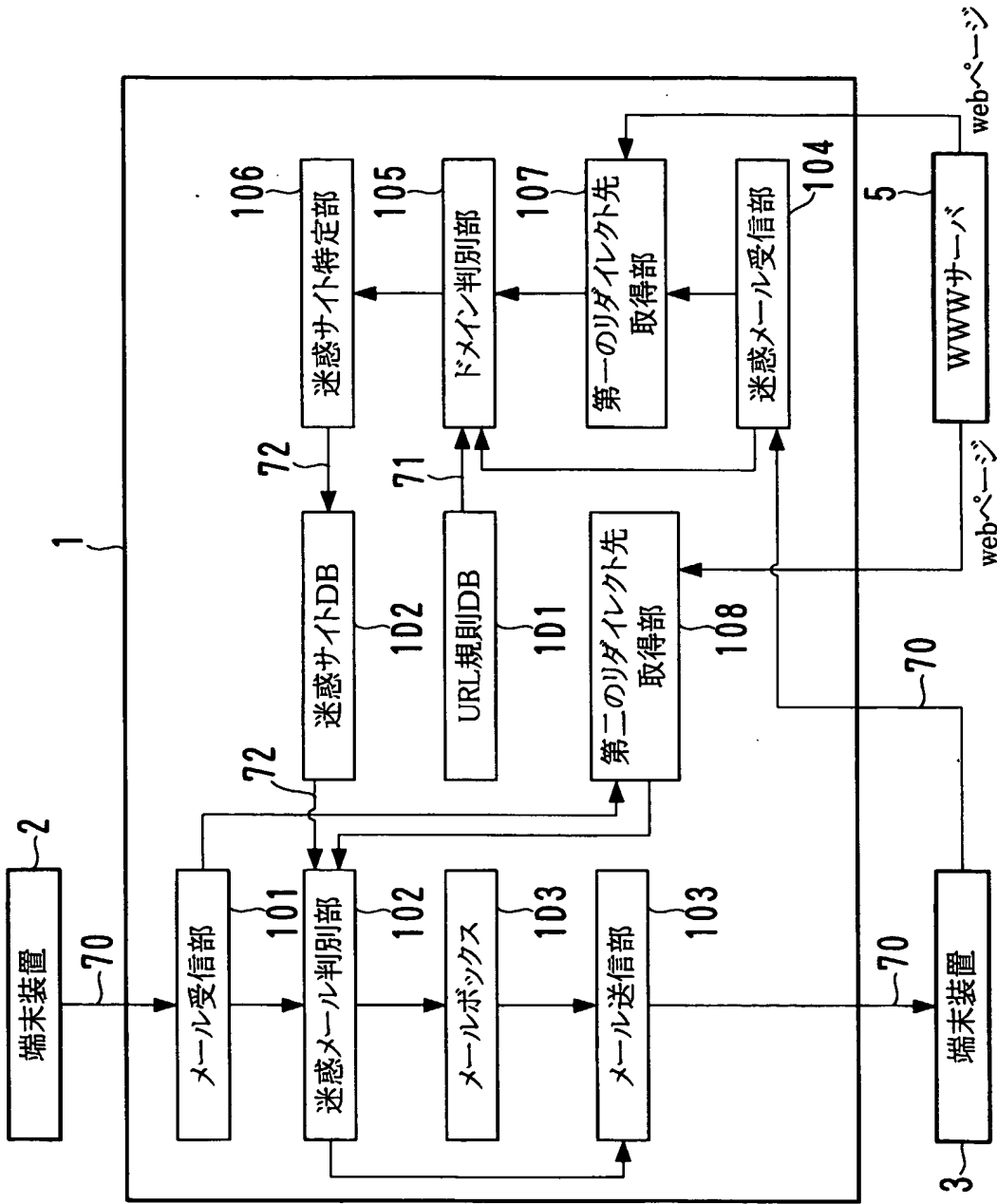
1

図4



5/12

図5

101

	ドメイン名	パターン	URLの形式
71a(71)	aaaaa.co.jp	E	独自ドメイン
71b(71)	bbbbbb.ne.jp	A	サイト名.bbbbb.ne.jp
71c(71)	cccc.ne.jp	B	cccc.ne.jp/サイト名
71d(71)	dddd.com	C	dddd.com/~サイト名
71e(71)	eeee.net	A	サイト名.eeeee.ne.jp
	⋮	⋮	⋮

6/12

図6

102

ユーザA 迷惑サイト	ユーザB 迷惑サイト	ユーザC 迷惑サイト
aaaaa.co.jp	aaaaa.co.jp	qqq.bbbbb.ne.jp
ppp.bbbbb.ne.jp	ppp.bbbbb.ne.jp	cccccc.ne.jp/sss
qqq.bbbbb.ne.jp	cccccc.ne.jp/rrr	cccccc.ne.jp/uuu
cccccc.ne.jp/rrr	ddddd.com/~ttt	vvv.eeeee.net
cccccc.ne.jp/sss		

72a(72)

72b(72)

72c(72)

7/12

図7

(a)

タイトル: マル秘情報
宛先: userA@mail.zzzzz.co.jp
差出人: xyz@hhhhh.co.jp

特別に、あなただけのために、出会いのマル秘情報をご案内します。詳しくは、

<http://www.ppp.bbbbb.ne.jp/top.html>

にアクセスしてください。

70a(70)

(b)

タイトル: マル秘情報
宛先: userA@mail.zzzzz.co.jp
差出人: xyz@jjjjj.co.jp

特別に、あなただけのために、出会いのマル秘情報をご案内します。詳しくは、

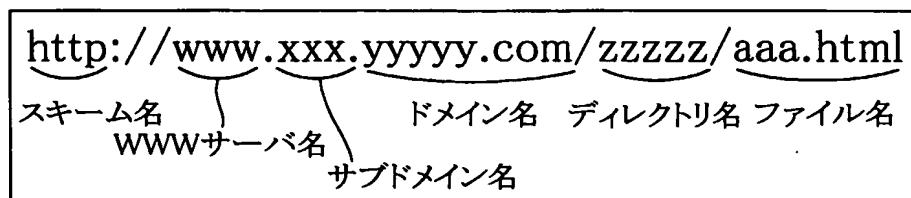
<http://ddddd.com/~abcd/index.html>

にアクセスしてください。

70b(70)

8/12

図8



9/12

図9

(a)

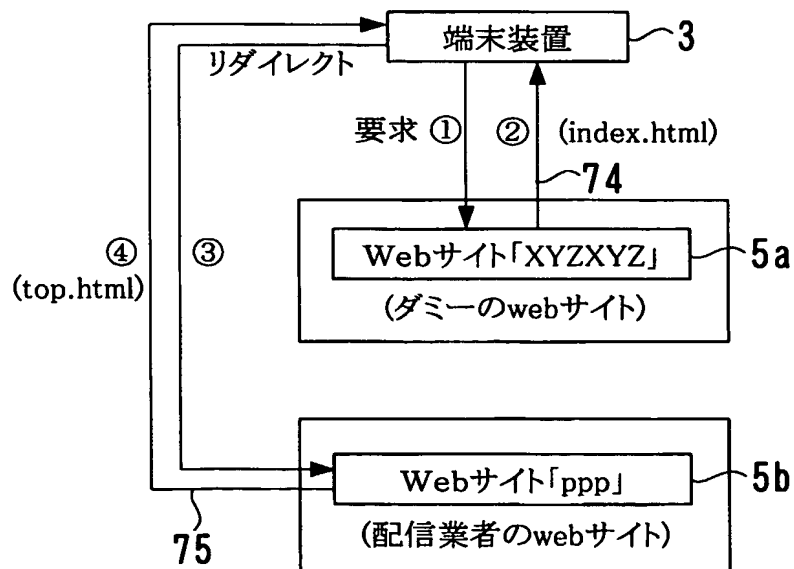
特別に、あなただけのために、出会いのマル秘情報をご案内します。詳しくは、

<http://yyyyyy.co.jp/~XYZXYZ/index.html>

にアクセスしてください。

70c

(b)



10/12

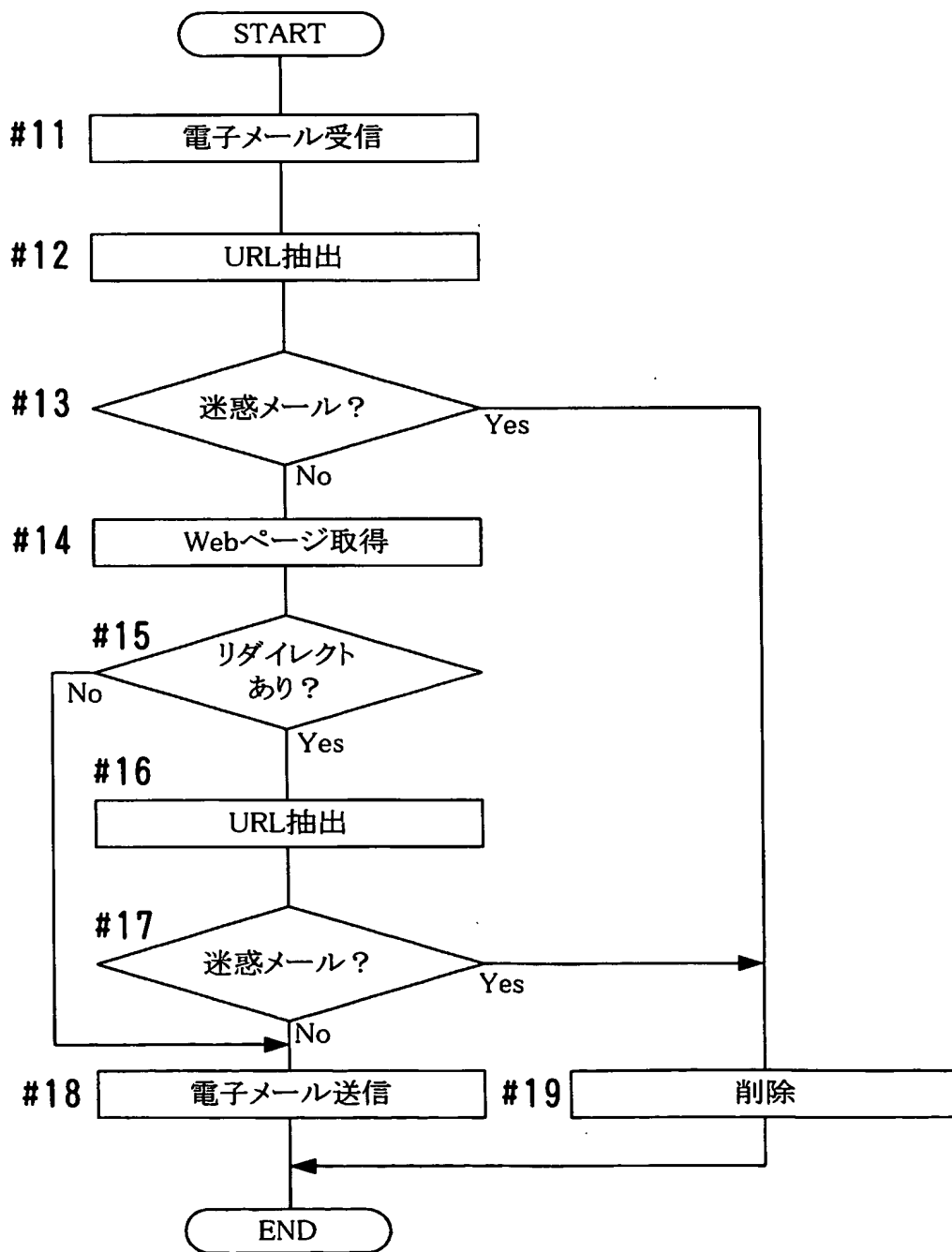
図10

```
<html>
<head>
<meta HTTP-EQUIV="Refresh" CONTENT="5; URL=http://
www.ppp.bbbbbb.ne.jp/top.html">
</head>
<body>
〇〇〇のページは移転しました。3秒後に自動的に新しいページ
に移動します。自動的に移動しない場合は、以下のリンクをクリッ
クしてください。<br>
<br>
<a href="http://www.ppp.bbbbbb.ne.jp/top.html">http://
www.ppp.bbbbbb.ne.jp/top.html</a><br>
</body>
</html>
```

C1

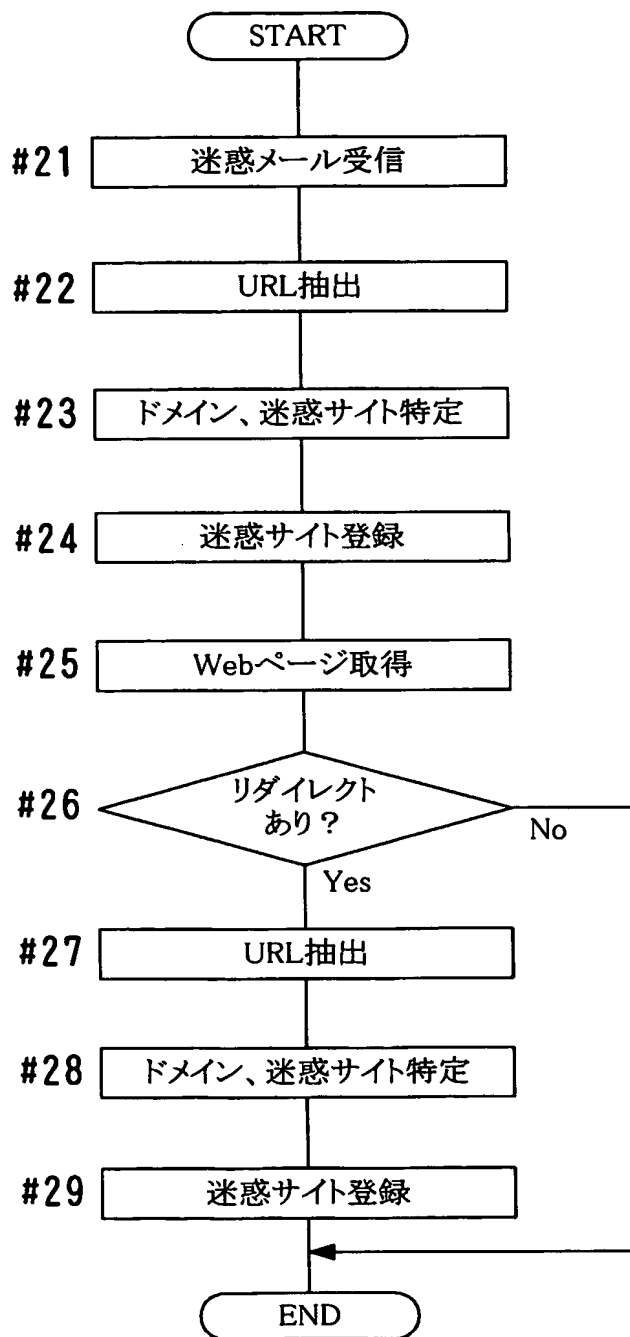
11/12

図11



12/12

図12



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP02/07402

A. CLASSIFICATION OF SUBJECT MATTER
Int.C1⁷ H04L12/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.C1⁷ H04L12/58, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/33188 A2 (Bright Light Technologies Inc.), 01 July, 1999 (01.07.99), Page 8, lines 14 to 27 & EP 1040584 A2 & US 6052709 A & JP 2001-527257 A & AU 1631199 A	1-6
X	GB 2350747 A (International Business Machines Corp.), 06 December, 2000 (06.12.00), & JP 2000-353133 A	1-6
X	JP 2000-10880 A (Ricoh Co., Ltd.), 14 January, 2000 (14.01.00), (Family: none)	1-6
X	"Denshi Mail no Tenso Anote Konote", ASCII, Vol.25, #7(July 2001), pages 348 to 352	1-6



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:
 "A" document defining the general state of the art which is not considered to be of particular relevance
 "E" earlier document but published on or after the international filing date
 "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 "O" document referring to an oral disclosure, use, exhibition or other means
 "P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
 "&" document member of the same patent family

Date of the actual completion of the international search
21 October, 2002 (21.10.02)Date of mailing of the international search report
05 November, 2002 (05.11.02)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl⁷ H04L 12/58

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl⁷ H04L 12/58, G06F 13/00

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	WO 99/33188 A2(BRIGHT LIGHT TECHNOLOGIES INC)1999.07.01 page 8 line 14 - page 8 line 27 & EP 1040584 A2 & US 6052709 A & JP 2001-527257 A & AU 1631199 A	1-6
X	GB 2350747 A(International Business Machines Corporation) 2000.12.06 & JP 2000-353133 A	1-6
X	JP 2000-10880 A(株式会社リコー)2000.01.14, (ファミリー無し)	1-6

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

21. 10. 02

国際調査報告の発送日

05.11.02

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

吉田 隆之



5X

9077

電話番号 03-3581-1101 内線 3594

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	"電子メールの転送あの手この手", ASCII Vol. 25 #7 (July 2001) p348-352	1-6

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.